CYBERCRIME PREVENTIE: Slachtoffer? Maak een afspraak met jouw politiezone

Verdachte mails? Stuur deze naar verdacht@safeonweb.be

CYBERSTALKING & CYBERPESTEN

PROBLEEM

- Iemand herhaaldelijk lastigvallen, bedreigen of vernederen via elektronische weg (e-mails, sms'en, foto's, commentaren, …).

PREVENTIEF

- Deel geen persoonlijke gegevens met onbekenden. Hou uw account zo privé mogelijk.
- Blijf steeds beleefd in uw communicatie. Wees voorzichtig met het gebruik van webcams.
- Negeer vriendschapsverzoeken van onbekenden.

SABOTAGE & VIRUSBESMETTING

PROBLEEM

- Uw computer wordt geblokkeerd en u heeft geen toegang meer tot uw bestanden.

PREVENTIEF

- Update regelmatig uw software. Installeer antivirus– en firewallsoftware.
- Maak regelmatig een back-up van uw bestanden.
- Gebruik een sterkt wachtwoord. Gebruik verificatie in 2 stappen (2FA).

RANSOMWARE

PROBLEEM

- Uw computer, mobiele apparaten of digitale bestanden worden vergrendeld en er wordt losgeld gevraagd om deze terug te ontgrendelen.

PREVENTIEF

- Update regelmatig uw software. Installeer antivirus– en firewallsoftware.
- Maak regelmatig een back-up van uw bestanden.
- Verwijder verdachte e-mails of berichten van onbekende afzenders.

SEXTORTION & SEXTORTIONSCAM

PROBLEEM

- Afpersing waarbij oplichters ermee dreigen om intieme beelden van uzelf te verspreiden indien u geen geldsom betaalt.
- Afpersing waarbij oplichters een e-mail sturen waarin wordt beweerd dat ze over intieme beelden van u beschikken die zullen worden verspreid indien u geen geldsom betaalt.

PREVENTIEF

- Negeer vriendschapsverzoeken van onbekenden.
- Deel geen seksueel getinte foto's of video's van uzelf.
- Negeer berichten waarin u wordt afgeperst (hacking/ intieme beelden).
- Scherm uw webcam af.

MISBRUIK BETAALKAARTEN & SKIMMING

PROBLEEM

- Uw pincode wordt achterhaald en vervolgens wordt uw bankkaart misbruikt.
- Uw bankkaartgegevens worden gekopieerd en misbruikt.

PREVENTIEF

- Bewaar geen pincode bij uw betaalkaarten. Controleer regelmatig uw rekeninguittreksels. Banken vragen nooit via e-mail vertrouwelijke informatie of pincodes op. Opteer voor een geldautomaat binnen i.p.v. een buitenautomaat. Let op voor verdachte voorwerpen rond de geldautomaat.
- Scherm steeds uw pincode af met de hand. Laat u niet afleiden tijdens de geldtransactie. Meer informatie op https://www.safeinternetbanking.be.

OPLICHTING VIA INTERNET & PHISHING

PROBLEEM

- Online oplichting via valse e-mails, websites of berichten.
- Online oplichting via een zoekertjessite.
- Oplichting waarbij uw bankkaartgegevens worden achterhaald en misbruikt.

PREVENTIEF

- Wees niet naïef, wat te mooi lijkt om waar te zijn, is dat meestal ook. Handel de verkoop niet af buiten de zoekertjessite. Betaal niet via een pakjes of transportbedrijf. Stuur nooit identiteitsdocumenten via e-mail door aan onbekenden. Opteer voor afhaling ter plaatse i.p.v. verzending.
- Vermijd betalingen via geldtransferagentschappen (Western Union, Moneygram). Verwijder verdachte e-mails of berichten van onbekende afzenders. Neem in geval van twijfel telefonisch contact op met uw bank. Klik nooit zomaar op verdachte links en bijlagen.
- Doe aankopen via betrouwbare websites (let op het slotje in de adresbalk). Geef nooit betaalkaartgegevens en/of pincodes door via e-mail.
- Geef nooit de pincode van uw betaal– of kredietkaart in op een website.

VALS PROFIEL

PROBLEEM

- Er wordt zonder uw toestemming een profiel aangemaakt met uw identiteitsgegevens en/of uw persoonlijke afbeelding.

PREVENTIEF

- Gebruik een sterk wachtwoord. Verspreid geen persoonlijke gegevens via internet. Deel een wachtwoord nooit met derden.
- Geef geen identiteitsdocumenten aan onbekenden. Let op met het verspreiden van persoonlijke gegevens via sociale media.

SCAMMING

PROBLEEM

- Oplichters nemen telefonisch contact met u op en doen zich voor als technici van een computerfirma (Microsoft, Apple, …). Ze vragen om bepaalde handelingen uit te voeren en/of uw bankgegevens door te geven.

PREVENTIEF

- Wantrouw telefoons van computerbedrijven die vertrouwelijke informatie of pincodes opvragen.
- Deel geen identiteits– en/of bankgegevens met onbekenden.

HACKING ACCOUNT

PROBLEEM

- Uw account werd gehackt waarbij er zonder uw medeweten berichten worden verstuurd naar uw contactpersonen, berichten of foto's op uw account worden geplaatst ...

PREVENTIEF

- Gebruik een sterk wachtwoord. Gebruik verificatie in 2 stappen (2FA).
- Gebruik voor elke account een ander wachtwoord. Deel een wachtwoord nooit met derden.
- Klik nooit zomaar op verdachte links en bijlagen. Verwijder e-mails of berichten van onbekende afzenders.

DENDERLEEUW HAALTERT DIENEN & BESCHERMEN

CYBERCRIME SLACHTOFFER: Maak een afspraak met jouw politiezone

Verdachte mails? Stuur deze naar verdacht@safeonweb.be

RANSOMWARE

PROBLEEM

- Uw computer, mobiele apparaten of digitale bestanden werden vergrendeld en er wordt losgeld gevraagd om deze terug te krijgen.

WAT TE DOEN

- Koppel het gehackte systeem los van het internet.
- Koppel alle andere toestellen los (USB-sticks, externe hardeschijven, …)/
- Bewaar zoveel mogelijk bewijsmateriaal (e-mails, schermafdrukken …).
- Ga niet in op de vraag om geld te betalen.
- Zoek gratis decryptiesleutels op: https://www.nomoreransom.org/.
- Laat uw toestel helemaal opnieuw installeren indien decryptie niet mogelijk is.

OPLICHTING VIA INTERNET & PHISHING

PROBLEEM

- U werd online opgelicht d.m.v. valse e-mail, website of bericht.
- U werd online opgelicht via een zoekertjessite.
- Uw bankkaartgegevens werden door derden achterhaald en misbruikt.

WAT TE DOEN

- Contacteer uw bank zo snel mogelijk om de transactie te blokkeren.
- Bel onmiddellijk CARD STOP: 070/344.344. Probeer een terugbetaling te bekomen via de bank.
- Contacteer de helpdesk van de zoekertjessite zelf.
- Maak melding van de (internet)fraude op: https://meldpunt.belgie.be

SEXTORTION & SEXTORTIONSCAM

PROBLEEM

- U werd overtuigd om intieme beelden van uzelf door te sturen en u wordt nu afgeperst om geld of bitcoins te betalen om verspreiding ervan te voorkomen.
- U ontvangt een e-mail waarin oplichters beweren dat ze intieme beelden van u bezitten en deze zullen verspreiden tenzij u geld of bitcoins betaalt.

WAT TE DOEN

- Ga niet in op de vraag om geld te betalen. Antwoord niet op de e-mail.
- Bewaar zoveel mogelijk bewijsmateriaal (e-mails, berichten, schermafdrukken …).
- Markeer het bericht als spam of ongewenst. Blokkeer de afzender.

SABOTAGE & VIRUSBESMETTING

PROBLEEM

- U kreeg een melding van een virus op uw computer.
- Uw computer werd geblokkeerd en u heeft geen toegang meer tot uw bestanden.

WAT TE DOEN

- Koppel het besmette systeem los van het internet.
- Installeer een virusscanner en zet deze onmiddellijk aan.
- Zoek antivirussoftware op: https://www.safeonweb.be/nl/heb-je-een-virus.
- Contacteer een gespecialiseerde computerzaak voor hulp.

MISBRUIK BETAALKAARTEN & SKIMMING

PROBLEEM

- Uw pincode werd achterhaald en vervolgens werd uw bankkaart misbruikt.
- Uw bankkaartgegevens werden gekopieerd en misbruikt.

WAT TE DOEN

- Bel onmiddellijk CARD STOP: 070/344.344.
- Neem zo snel mogelijk contact op met uw bank.
- Betwist de geldtransactie(s) op: https://www.mijnkaart.be
- Probeer een terugbetaling te bekomen via de bank.

VALS PROFIEL

PROBLEEM

- Er werd een vals profiel aangemaakt met uw identiteitsgegevens en/of uw persoonlijke afbeelding.

WAT TE DOEN

- Maak melding bij de beheerder van de website.
- Bewaar zoveel mogelijk bewijsmateriaal (accountnaam, afbeeldingen, schermafdrukken …).

CYBERSTALKING & CYBERPESTEN

PROBLEEM

- U wordt herhaaldelijk via elektronische weg (e-mails, sms-en, foto's, commentaren …) bedreigd, vernederd of lastiggevallen.

WAT TE DOEN

- Bewaar zoveel mogelijk bewijsmateriaal (e-mails, scherm-afdrukken, accountnaam, mailheaders …).
- Maak melding bij de beheerder van de website.

SCAMMING

PROBLEEM

- U werd opgebeld door oplichters die zich voordeden als technici van een computerfirma (Microsoft, Apple, …) en zij vroegen u bepaalde handelingen uit te voeren en/of uw bankgegevens door te geven.

WAT TE DOEN

- Bel onmiddellijk CARD STOP: 070/344.344.
- Neem zo snel mogelijk contact op met uw bank.
- Probeer een terugbetaling te bekomen via de bank.
- Bewaar zoveel mogelijk bewijsmateriaal (e-mails, telefoonnummers, betalingsbewijs …).

HACKING ACCOUNT

PROBLEEM

- Uw account werd gehackt waarbij er zonder uw medeweten berichten werden verstuurd naar uw contactpersonen, berichten of foto's op uw account werden geplaatst …

WAT TE DOEN

- Verander onmiddellijk uw wachtwoord als u nog toegang heeft tot uw account.
- Contacteer de helpdesk van de website zelf indien u geen toegang meer heeft.
- Koppel het gehackte systeem los van het internet.

DENDERLEEUW HAALTERT
DIENEN & BESCHERMEN